**Riadenie kapacity systémov a služieb**

**(smernica)**

***PETAN parket, s.r.o., M.R. Štefánika 314, 956 18 Bošany, IČO: 50 341 189***

Táto interná smernica je spracovaná na základe dobrej praxe a reflektuje pravidlá a postupy v kontexte požiadaviek medzinárodnej normy STN ISO/IEC 27001:2014 v oblasti riadenia kapacít (Príloha A.12 Bezpečnosť prevádzky, A.12.1 Prevádzkové postupy a zodpovednosť, A.12.1.3 Riadenie kapacít). Smernica vychádza tiež z požiadaviek legislatívy v oblasti informačnej a kybernetickej bezpečnosti.

|  |  |
| --- | --- |
| **Číslo dokumentu** | *002/2024* |
| **Vydanie/Dátum** | *Vydanie č. 1/10.04.2024* |
| **Revízia/Dátum** | *Bez revízie/10.04.2024* |
| **Počet strán** | *11* |

|  |  |  |
| --- | --- | --- |
| **Autor dokumentu** | *Štandart BPPO s. r. o.* |  |
| **Vlastník dokumentu** | *PETAN parket, s.r.o.* |  |
| **Schválil** | *Kvetoslava Turčeková, konateľ* | *Podpis* |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Kľúčové súvisiace predpisy a normy**

1. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
2. Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení [najmä však § 16 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. l) zákona – fyzická bezpečnosť sietí a informačných systémov]
3. Súbor medzinárodných noriem radu ISO/IEC 27000
4. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe
5. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (najmä však Príloha č. 2, bod F. Bezpečnosť pri prevádzke informačných systémov a sietí, bod K. Zaznamenávanie udalostí a monitorovanie, bod L. Fyzická bezpečnosť a bezpečnosť prostredia)
6. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z., ktorou sa mení a dopĺňa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy

**Čl. 1**

**Úvod**

1. Organizácia na základe monitorovania svojich sietí a informačných systémov vrátane kritickej infraštruktúry a kľúčových personálnych zdrojov identifikuje potenciálne miesta preťaženia a závislosti od kľúčového personálu. Tie pre organizáciu predstavujú hrozbu pre bezpečnosť jej aktív alebo pre ňou poskytované produkty a služby.
2. Pre tento účel organizácia spracovala túto smernicu pre riadenie kapacity svojich systémov a služieb.
3. V predmetnej oblasti organizácia zaviedla schému bezpečnostných rolí, pričom v oblasti riadenia kapacít platia nasledovné princípy:
4. vlastník aktíva – je zodpovedný za riadenie kapacít,
5. manažér informačnej bezpečnosti – aktívne spolupracuje pri návrhu, implementácii a riadení kapacít,
6. bezpečnostný výbor organizácie – aktívne spolupracuje pri návrhu, implementácii a riadení kapacít,
7. vedúci manažér – aktívne spolupracuje pri návrhu, implementácii a riadení kapacít,
8. organizačný útvar IT – je primárne zodpovedný za vykonanie riadenia kapacít,
9. organizačný útvar obstarávania a nákupu tovarov a služieb – aktívne spolupracuje pri návrhu, implementácii a riadení kapacít,
10. organizačný útvar bezpečnosti – aktívne spolupracuje pri návrhu, implementácii a riadení kapacít.

**Čl. 2**

**Riadenie kapacít systémov a služieb**

1. Organizácia definovala kapacitné požiadavky zohľadňujúce kritickosť používaných sietí a informačných systémov. Zaviedla ich monitorovanie, aby sa zabezpečila ich dostupnosť a efektívnosť.
2. Organizácia zabezpečuje, aby odhady budúcej kapacity vrátane redundancie brali do úvahy nové technické a technologické požiadavky na siete a informačné systémy vrátane sledovania budúcich trendov dostupnosti infraštruktúry organizácie.
3. Organizácia venuje špeciálnu pozornosť najmä zdrojom s vysokými obstarávacími nákladmi a dlhou obstarávacou lehotou.
4. Zodpovední manažéri (vlastníci siete alebo informačného systému) sú zodpovední za priebežnú identifikáciu trendov v oblasti používaných a plánovaných aplikácií, softvérového a hardvérového vybavenia, ako aj nástrojov riadenia sietí a informačných systémov. Zodpovední manažéri sú povinní používať získané informácie na identifikovanie a prevenciu potenciálnych miest preťaženia sietí a informačných systémov a ich závislosť na kľúčovom personáli (z pohľadu, že personálne zdroje môžu potenciálne predstavovať hrozbu pre bezpečnosť konkrétnej siete alebo informačného systému, resp. pre služby používateľom).
5. Organizácia vyhlasuje, že poskytnutie dostatočnej kapacity dosahuje aj rastom kapacity alebo znížením požiadaviek, a to najmä vymazávaním nepotrebných údajov (uvoľňovanie priestoru na záznamovom disku), vyraďovaním nepotrebných aplikácií, systémov, databáz alebo celých produkčných alebo vývojových prostredí, optimalizáciou procesov, aplikačnej logiky alebo databázových dopytov, resp. zakázaním alebo obmedzením šírky pásma pre zdroje náročné na služby (ak tie nie sú kritické – napr. posielanie videosúborov a pod.).
6. Organizácia riadi kapacity aj z pohľadu počtu zamestnancov, počtu súčasne pripojených používateľov, ako aj počtu pripojení do sietí a informačných systémov v jednom momente.

**Čl. 3**

**Analýza funkčného dopadu**

1. Plánovanie prevádzky kritických procesov organizácie, samotnej činnosti sietí a informačných systémov, ako aj následnej obnovy sietí a informačných systémov v prípade ich narušenia, resp. poškodenia vychádza z požiadaviek a potrieb konkrétnych používateľov na prevádzku sietí a informačných systémov a na dostupnosť údajov v nich.
2. Organizácia spracovala **analýzu funkčného dopadu**, ktorá pozostáva z hodnotenia dopadu na reálnu činnosť organizácie *PETAN parket, s.r.o.* spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy a spôsobiť ohrozenie alebo narušenie kontinuity jeho poskytovanej služby.
3. Analýza funkčného dopadu *je súčasťou* riadenia aktív, hrozieb a rizík.
4. V **analýze funkčného dopadu** organizáciaidentifikovala požiadavky na obnovu konkrétnej siete alebo informačného systému. V analýze sú uvedené a pravidelne *minimálne raz ročne* preskúmavané spôsob a metóda jej vykonania, minimálne kapacitné požiadavky na siete a informačné systémy, spôsob zabezpečenia ich redundancie, typ chránených dát, spôsob ochrany infraštruktúry, zodpovedná osoba a jej miera zodpovednosti, perióda vykonávania analýzy dopadov, v prípade zálohovania aj použitý zálohovací hardvér, typ zálohy, ako aj určenie zálohovaných serverov (údajov).

**Čl. 4**

**Kapacitný plán**

1. Organizácia pre svoje kritické siete a informačné systémy, kritické priestory a kľúčové ľudské zdroje vypracovala **Kapacitný plán** na určené obdobie *(napr. na tri roky)*. Tento plán preskúmava pravidelne *minimálne raz ročne* manažér informačnej bezpečnosti so zámerom zistenia ich aktuálneho stavu a zabezpečenia vhodnej kapacity a efektívnej funkčnosti počas nepriaznivých situácií.
2. V **Kapacitnom pláne** sa organizácia sústredila na definovanie minimálnej úrovne kapacity sietí a informačných systémov potrebných na svoju prevádzkovú činnosť a vývoj i testovanie poskytovaných produktov a služieb. Zároveň v ňom spracovala oblasť ochrany záznamov informácií formou definovania bezpečnostných opatrení s dôrazom na ich implementáciu pre účely ochrany pred neautorizovanými zmenami a prevádzkovými problémami v súvislosti s prostriedkami a tvorbu záznamov.
3. Pre udržanie procesov informačnej a kybernetickej bezpečnosti je vlastník aktíva v spolupráci s manažérom informačnej bezpečnosti povinný vypracovať, zaviesť a udržiavať procesy, postupy a opatrenia na zabezpečenie požadovanej úrovne dostatočnej kapacity a kontinuity činností. Súčasťou **Kapacitného plánu** je stratégia obnovy sietí a informačných systémov tak, aby bola zabezpečená ich prevádzkyschopnosť v kontexte včasného plánovania dostatočných kapacít.
4. Procesy informačnej a kybernetickej bezpečnosti sú súčasťou systému riadenia kontinuity činností v organizácii. Všetky významné procesy informačnej a kybernetickej bezpečnosti musia byť v adekvátnej miere zachované aj v mimoriadnych situáciách, napr. počas krízy alebo katastrofy. **Kapacitný plán** je preto procesne prepojený s dokumentáciou riadenia kontinuity a v oblasti informačných a komunikačných technológií sa v ňom uvádzajú požiadavky a parametre procesov v prípade narušenia prevádzky, minimálne však cieľový čas obnovenia (Recovery Time Objective – RTO), maximálna doba výpadku (Maximum tolerable outage – MTO, resp. Maximum tolerable period of disruption – MTPD) a cieľový bod obnovenia (Recovery Point Objective – RPO), a to pre každý kritický informačný systém alebo sieť zvlášť.
5. **ZÁLOHOVANIE:** V **Kapacitnom pláne** organizácia v súvislosti so záznamovými médiami (prostriedky na tvorbu záznamov) rozpracovala oblasť zmien typov správ, resp. hlásení, ktoré sa zaznamenávajú, oblasť editovania alebo mazania súborov záznamu, ako aj oblasť prekročenia kapacity záznamových médií, čo môže spôsobiť zlyhanie zaznamenávania udalostí alebo prepísanie v minulosti zaznamenaných udalostí. Predmetná oblasť zálohovania sa riadi čl. 8 tejto smernice.
6. **ARCHIVÁCIA:** V oblasti monitorovania zapracovala organizácia do **Kapacitného plánu** aj oblasť archivácie. To z dôvodu, že pri niektorých auditných záznamoch sa môže vyžadovať ich archivácia v súvislosti s uplatnením politiky uchovávania záznamov alebo v súvislosti s požiadavkami kladenými na zhromažďovanie a uchovávanie dôkazných materiálov. Predmetná oblasť archivácie sa riadi čl. 8 tejto smernice.
7. **Kapacitný plán** je úzko prepojený s **analýzou rizík**. Konkrétne na hrozby a zraniteľnosti v oblasti zlyhania **dostupnosti informačných služieb** (spôsobené vyčerpaním zdrojov, najmä však nedostatočnou kapacitou sietí alebo informačných systémov či rôznych typov kybernetických útokov), resp. **nedostupnosťou aktív** (z dôvodu neexistencie, krádeže, zničenia, stratenia, uzamknutia v nedostupných priestoroch a pod.).

**Čl. 5**

**Riadenie kapacít podporných služieb**

1. Organizácia zabezpečuje, že v oblasti podporných služieb (napr. dodávky elektrickej energie, telekomunikačné služby, dodávky vody, dodávky plynu, odvoz a separácia odpadu, prevádzky vzduchotechniky a klimatizácie a pod.) pri plánovaní minimálnych kapacít a redundancie tieto musia vyhovovať špecifikáciám výrobcov zariadení a miestnym právnym požiadavkám a musia byť pravidelne prehodnocované a testované na funkčnosť, bezpečnosť, prevádzkyschopnosť, legislatívny súlad, resp. vlastnú kapacitu tak, aby splnili potreby realizovaných služieb a dodávaných produktov organizácie a tiež prepojení s ostatnými podpornými službami v kontexte externých a interných súvislostí organizácie.
2. Riadenie dostupnosti elektrickej energie:
3. informačné a komunikačné technológie a zariadenia organizácie musia byť chránené pred výpadkami napájania a inými prerušeniami spôsobenými poruchami napájacích zariadení,
4. núdzové vypínače sa musia nachádzať v blízkosti núdzových východov s vybavením, ktoré uľahčia rýchle vypnutie v prípade núdze,
5. musí byť zabezpečené núdzové osvetlenie v prípade výpadku hlavného prúdu,
6. neprerušiteľný zdroj napájania (UPS) a *dieselové generátory* sa musia inštalovať na podporu nepretržitej podpory zariadení podporujúcich kritické prevádzkové a obchodné procesy,
7. telekomunikačné vybavenie musí byť spojené s poskytovateľom telekomunikačných služieb *najmenej dvoma rôznymi trasami*, aby sa zabránilo zlyhaniu jednej spojovacej cesty.

**Čl. 6**

**Riadenie konfigurácie a údržby z pohľadu zabezpečenia kapacít**

1. Servery a kritické sieťové informačné aktíva organizácie sú umiestnené výhradne v prostredí s kontrolovaným vstupom.
2. Konfigurácia operačných systémov je v zhode s implementovanými procedúrami v oblasti riadenia kapacít v prostredí organizácie.
3. Konfigurácia záloh je riadená a je zabezpečené, že pre všetky kritické informačné aktíva v prostredí organizácie sú zálohy trvale udržiavané.
4. Všetky servery, kritické informačné aktíva a pracovné stanice v prostredí organizácie majú nainštalovaný schválený softvér a schválený antivírusový softvér.
5. Bezpečnostné záplaty sú inštalované ihneď po identifikácii ich sprístupnenia.
6. Všetky nepoužívané služby a aplikácie sú defaultne vypnuté a znefunkčnené.
7. Monitorovacie a logovacie služby sú aktivované v kontexte požiadaviek pre monitorovanie prevádzky v sieťach a informačných systémoch.
8. Riadenie prístupov administrátorov a privilegovaných administrátorov k serverom organizácie a ovládanie sieťových zariadení v prostredí organizácie je v kontexte nastavených bezpečnostných procesov a takýto prístup je povolený výlučne administrátorom informačných aktív v rámci dodržiavania princípu minimálnych prístupových práv.
9. V oblasti údržby sietí a informačných systémov vykonáva organizácie procesy údržby aj pri zmenách operačných systémov. Realizuje revíziu kritických aplikácií a testovanie, aby výsledok zmien nemal negatívny dopad na prevádzku organizácie alebo na kybernetickú bezpečnosť.
10. Organizácia pravidelne *na mesačnej báze* preveruje procedúry riadenia a integrity aplikácií, zaisťuje včasnú komunikáciu o zmenách operačných systémov a zaisťuje vykonanie zmien v kapacitnom pláne a v plánoch kontinuity prevádzky.

**Čl. 7**

**Riadenie zmien infraštruktúry z pohľadu zabezpečenia kapacít**

1. Pre riadenie zmien infraštruktúry organizácia identifikovala a dokumentačne zaznamenala interné procesy pre významné zmeny v plánovaní kapacít, testuje ich a zhodnocuje bezpečnostné dôsledky takýchto zmien.
2. Organizácia spracovala formálny postup schvaľovania navrhnutých zmien, v rámci ktorého overuje plnenie požiadaviek informačnej a kybernetickej bezpečnosti a oznamuje podrobnosti zmien všetkým relevantným osobám (rolám v organizácii).
3. Organizácia má vypracované havarijné postupy, ktoré pokrývajú kroky a zodpovednosti za predčasné ukončenie a obnovu po neúspešných zmenách a výskyte nepredvídaných udalostí. Cieľom havarijných postupov je zaistiť uspokojivý dohľad nad všetkými zmenami aktív organizácie. Po vykonaní zmien organizácia uchováva záznamy pre účel bezpečnostného auditu.
4. Kapacita a dostupnosť kritickej infraštruktúry:
5. vlastníci aktív a administrátori sietí a informačných systémov organizácie sú zodpovední za identifikovanie požiadaviek na kapacitu a dostupnosť jednotlivých sietí a informačných systémov, kritických komponentov infraštruktúry organizácie, služieb alebo aplikácií, ako aj preverenie možností aktuálnej garancie požadovanej úrovne kapacity a dostupnosti,
6. v prípade, že požadovaná úroveň kapacity a dostupnosti sietí a informačných systémov nie je zaručená v súčasnej architektúre technických a technologických riešení, sú zvážené možnosti vytvorenia redundantnej architektúry alebo ďalšie možnosti pre dosiahnutie požadovanej úrovne kapacity a dostupnosti.

**Čl. 8**

**Zálohovanie, archivácia a obnova z pohľadu riadenia kapacít**

1. Vlastník aktíva a administrátor technických a technologických zariadení v organizácii (minimálne však kritickej infraštruktúry) je povinný vykonávať zálohovanie a archiváciu údajov podľa zavedených organizačných inštrukcií a procesov pre vytváranie záložných kópií dôležitých informácií a softvéru *na dennej báze*.
2. Vlastník aktíva a administrátor technických a technologických zariadení v organizácii je povinný úzko spolupracovať s manažérom informačnej (kybernetickej) bezpečnosti na vypracovaní organizačných postupov a inštrukcií pre riadenie kapacít, vytváranie záloh a obnovu dát, ktoré musia obsahovať požiadavky organizácie na dostatočné kapacity a zálohovanie (najmä parametre RTO a RPO), retenciu údajov, testovanie záloh, ako aj požiadavky na adekvátnu ochranu záložných médií.
3. Vlastník aktíva a administrátor technických a technologických zariadení v organizácii je povinný *minimálne raz za rok* otestovať obnovu dát podľa definovanej procedúry.
4. Médiá so záložnými údajmi musia byť uložené v inej fyzickej miestnosti alebo lokalite. V prípade, ak nie je toto bezpečnostné opatrenie možné splniť, musia byť média s archívnymi údajmi uložené oddelene od médií so záložnými údajmi tak, aby sa v maximálnej možnej miere zamedzilo súčasnému zničeniu záložných aj archívnych médií v prípade mimoriadnej situácie alebo ich odcudzenia, či straty prekonaním jednej a tej istej prekážky.
5. Zálohovanie a obnova je definovaná procedúrami pre každý systém zvlášť a je uchovávaná v digitálnej a papierovej podobe a je za ne zodpovedný vlastník aktíva a administrátor technických a technologických zariadení v organizácii.

**Čl. 9**

**Bezpečnostné pravidlá pre riadenia kapacít**

Organizácia implementovala a riadi nasledovné bezpečnostné pravidlá a princípy v oblasti riadenia kapacít:

1. Siete a informačné systémy vrátane kritickej infraštruktúry musia byť monitorované tam, kde je to technicky možné, s cieľom identifikácie kapacitných požiadaviek tak, aby nedošlo ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche ich funkčnosti.
2. Administrátor siete alebo informačného systému zodpovedá za správnu implementáciu, údržbu a správu monitorovacích nástrojov a utilít v komplexnej infraštruktúre organizácie pre systémy v jeho zodpovednosti.
3. Riadenie kapacít je v organizácii sledované oficiálne schváleným nástrojom na monitoring a sledovanie kapacít, kde musia byť monitorované minimálne nasledovné parametre systému:
4. sieťová prevádzka,
5. vyťaženosť systémov,
6. voľné miesto lokálnych úložísk zariadení alebo systémov,
7. monitoring hardvérových komponentov.
8. Administrátori sietí a informačných systémov a sieťoví špecialisti sú povinní sledovať kapacity sietí a informačných systémov, spravovať uvoľňovanie miesta na pevných diskoch, optimalizovať dávkové procesy, optimalizovať databázové dopyty a nastavovať reštrikcie nekritických služieb náročných na zdroje.

**Čl. 10**

**Záverečné ustanovenia**

1. Táto smernica a z nej vyplývajúca súvisiaca bezpečnostná dokumentácia zavedená v organizácii nadobúda účinnosť schválením predpísanými postupmi.
2. Odborný výklad tejto smernice je oprávnený podávať a kontrolou jej dodržiavania formou auditov je konateľ organizácie Kvetoslava Turčeková.
3. Za dodržiavanie tejto smernice zodpovedá konateľ organizácie Kvetoslava Turčeková.
4. Ak v priebehu účinnosti tejto smernice dôjde k zmenám platných ustanovení, noriem, predpisov a internej dokumentácie, s ktorými bude táto smernica v nesúlade, vedenie organizácie ju zmení vydaním ďalšej nasledujúcej verzie.

Bošany, dňa...... Schválil: .............................................

konateľ organizácie

Kvetoslava Turčeková